

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日            2 0 0 3 年   3 月 3 1 日  
Date of Application:

出 願 番 号            特 願 2 0 0 3 - 0 9 5 6 7 1  
Application Number:  
[ST. 10/C]:            [ J P 2 0 0 3 - 0 9 5 6 7 1 ]

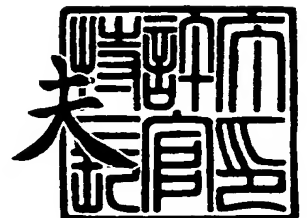
出   願   人            株 式 会 社 東 芝  
Applicant(s):



2 0 0 3 年   7 月 1 8 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



【書類名】 特許願

【整理番号】 A000205954

【提出日】 平成15年 3月31日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 15/00

【発明の名称】 オフライン情報を利用したデバイス認証装置及びデバイス認証方法

【請求項の数】 16

【発明者】

    【住所又は居所】 東京都青梅市末広町 2 丁目 9 番地 株式会社東芝青梅事業所内

    【氏名】 金澤 浩二

【発明者】

    【住所又は居所】 東京都青梅市末広町 2 丁目 9 番地 株式会社東芝青梅事業所内

    【氏名】 馬渡 正彦

【特許出願人】

    【識別番号】 000003078

    【氏名又は名称】 株式会社 東芝

【代理人】

    【識別番号】 100058479

    【弁理士】

    【氏名又は名称】 鈴江 武彦

    【電話番号】 03-3502-3181

【選任した代理人】

    【識別番号】 100091351

    【弁理士】

    【氏名又は名称】 河野 哲

## 【選任した代理人】

【識別番号】 100088683

【弁理士】

【氏名又は名称】 中村 誠

## 【選任した代理人】

【識別番号】 100108855

【弁理士】

【氏名又は名称】 蔵田 昌俊

## 【選任した代理人】

【識別番号】 100084618

【弁理士】

【氏名又は名称】 村松 貞男

## 【選任した代理人】

【識別番号】 100092196

【弁理士】

【氏名又は名称】 橋本 良郎

## 【手数料の表示】

【予納台帳番号】 011567

【納付金額】 21,000円

## 【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 オフライン情報を利用したデバイス認証装置及びデバイス認証方法

【特許請求の範囲】

【請求項 1】 通信機能を持つ機器に設けられるデバイス認証装置であって

他の機器によって可搬型の記録媒体に記録された認証データを読み込む読み込み手段と、

前記読み込み手段により読み込まれた前記認証データを記録する記録手段と、

前記記録手段に記録された前記認証データを用いて、前記他の機器との間で相互認証処理を行なう認証手段と

を具備したことを特徴とするデバイス認証装置。

【請求項 2】 通信機能を持つ機器に設けられるデバイス認証装置であって

認証データを生成する生成手段と、

前記生成手段により生成した前記認証データを可搬型の記録媒体に記録する認証データ記録手段と、

前記記録媒体に記録された前記認証データを記録する記録手段と、

前記記録手段により記録された前記認証データを用いて、前記可搬型の記録媒体から前記認証データを読み込んだ他の機器との間で相互認証処理を行なう認証手段と

を具備したことを特徴とするデバイス認証装置。

【請求項 3】 前記記録手段は、

不揮発性の記録媒体によって前記認証データを記録することを特徴とする請求項 1 または請求項 2 記載のデバイス認証装置。

【請求項 4】 前記認証手段は、

前記認証データに含まれる有効期間を示すデータをもとに、有効期間中にあるかを判別する判別手段と、

前記判別手段によって有効期間が経過したと判別された場合に、前記認証デー

タを無効にする無効手段とを具備したことを特徴とする請求項 1 記載のデバイス認証装置。

【請求項 5】 前記生成手段は、  
有効期間を示すデータを含む認証データを生成することを特徴とする請求項 2 記載のデバイス認証装置。

【請求項 6】 前記認証手段は、  
相互認証処理の実行回数を記憶する回数記憶手段と、  
前記認証データに含まれる有効回数を示すデータをもとに、有効期間中にあるかを判別する判別手段と、  
前記判別手段によって有効期間中にあると判別された場合に、前記認証データを無効にする無効手段とを具備したことを特徴とする請求項 1 記載のデバイス認証装置。

【請求項 7】 前記生成手段は、  
有効期間を示すデータを含む認証データを生成することを特徴とする請求項 2 記載のデバイス認証装置。

【請求項 8】 前記認証手段は、  
他の機器からの認証要求を受信する第 1 受信手段と、  
前記第 1 受信手段に受信された認証要求に対して、前記認証データを用いて生成されるデータを前記他の機器に対して送信する第 1 送信手段と  
を具備したことを特徴とする請求項 1 記載のデバイス認証装置。

【請求項 9】 前記認証手段は、  
前記他の機器に対して認証要求を送信する第 2 送信手段と、  
前記第 2 送信手段によって送信した送信要求に応じて、前記他の機器から送信されるデータを受信する第 2 受信手段と、  
前記第 2 受信手段によって受信したデータが前記認証データを用いて生成されているかを判別する判別手段と  
を具備したことを特徴とする請求項 2 記載のデバイス認証装置。

【請求項 10】 前記認証手段は、  
前記認証データを用いて生成されるデータを前記他の機器に対して送信する第

3 送信手段と、

前記他の機器から送信されるデータを受信する第3受信手段と、

前記第3受信手段によって受信したデータが前記認証データを用いて生成されているかを判別する判別手段と

を具備したことを特徴とする請求項1または請求項2記載のデバイス認証装置。

【請求項11】 前記可搬型の記録媒体は、記録されたデータの正当性が保証される記録媒体であることを特徴とする請求項1または請求項2記載のデバイス認証装置。

【請求項12】 前記生成手段は、

所有者データを取得する取得手段と、

前記所有者データをもとに認証データを生成する認証データ生成手段とを具備したことを特徴とする請求項2記載のデバイス認証装置。

【請求項13】 前記取得手段は、

所有者の生体情報を入力する生体情報入力手段を有することを特徴とする請求項13記載のデバイス認証装置。

【請求項14】 前記取得手段は、

所有者データを入力する入力手段と、

前記入力手段によって入力された前記所有者データの正当性を確認する所有者データ確認手段とを有することを特徴とする請求項13記載のデバイス認証装置。

【請求項15】 通信機能を持つ機器におけるデバイス認証方法であって、

第1の機器において、認証データを生成して記録しておくと共に、可搬型の記録媒体に記録し、

第2の機器において、前記第1の機器によって可搬型の記録媒体に記録された認証データを前記可搬型の記憶媒体から読み込んで記録し、

前記第1の機器と前記第2機器の間で、それぞれに記憶された前記認証データを用いて相互認証処理を行なうことを特徴とするデバイス認証方法。

【請求項16】 前記相互認証処理では、

前記第1の機器において前記認証データをもとに生成した第1のデータを前記

第2の機器に送信し、

前記第2の機器において前記認証データをもとに生成した第2のデータを前記第1の機器に送信し、

前記第1の機器において前記第2の機器から送信されたデータが前記認証データを用いて生成されているかを判別し、

前記第2の機器において前記第1の機器から送信されたデータが前記認証データを用いて生成されているかを判別する

ことを特徴とする請求項15記載のデバイス認証方法。

**【発明の詳細な説明】**

**【0001】**

**【発明の属する技術分野】**

本発明は、通信機能を有する機器におけるデバイス認証装置及びデバイス認証方法に関する。

**【0002】**

**【従来の技術】**

従来、ライセンス技術を使用してライセンスされた限られた機器間で通信をする場合、例えばデジタルコンテンツを提供するサーバとコンテンツの提供先となるクライアント機器が通信をする場合には、クライアント機器がライセンスされた正しい機器であることを確認するために、通信を行なう前に認証処理を行っている。認証処理によってライセンスされた機器であることが確認されると、例えば暗号化されたコンテンツを解除するためのキー（データ）が交換され、クライアント機器においてコンテンツを扱うことができるようになる。

**【0003】**

しかし、従来の認証処理では、通信相手の機器がライセンスされた技術を使用した正しい機器であるかどうかだけしか確認することはできない。このため、ライセンスされた機器の中でさらに限られた特定の機器のみを対象として通信することができない。

**【0004】**

例えば、機器間が無線通信によって接続される場合、A家内に設置された機器

にのみ通信を許可しようとしても、隣接しているB家に設置されているライセンスされた機器がA家の機器と無線通信が可能であれば、B家の機器においても何の制限も無く通信が可能となってしまう。従って、デジタルコンテンツの提供先として意図していない機器に対してもコンテンツが提供されてしまうことになる。

#### 【0005】

従来、ネットワークにログインする際に不正ログインを防止するために、ログイン情報を可搬の記録媒体に記録しておき、この記録媒体を用いてログインする方法が考えられている（例えば、特許文献1）。特許文献1のログイン方法では、ログイン情報（ユーザ情報）が記録された記録媒体を装着したクライアントPCのみがログインされネットワークを利用することができる。

#### 【0006】

##### 【特許文献1】

特開 2002-215590号公報

#### 【0007】

##### 【発明が解決しようとする課題】

このように従来では、機器間で認証処理を実行することで、ライセンス技術を使用してライセンスされた限られた機器のみを対象として接続相手とする機器を制限することができるが、ライセンスされた機器中でさらに限られた機器のみを通信相手として制限することができなかった。

#### 【0008】

本発明は前記のような事情を考慮してなされたもので、認証時に使用される認証データを可搬型の記憶媒体を通してオフラインで認証機器側から被認証機器側へ相互認証処理が行なわれる前に渡すことにより、ライセンスされた正しい機器のうち、事前に認証機器側からオフラインで認証データを取得した被認証機器だけを接続可能にするデバイス認証装置及びデバイス認証方法を提供することを目的とする。

#### 【0009】

##### 【課題を解決するための手段】



本発明は、通信機能を持つ機器に設けられるデバイス認証装置であって、他の機器によって可搬型の記録媒体に記録された認証データを読み込む読み込み手段と、前記読み込み手段により読み込まれた前記認証データを記録する記録手段と、前記記録手段に記録された前記認証データを用いて、前記他の機器との間で相互認証処理を行なう認証手段とを具備したことを特徴とする。

#### 【0010】

また本発明は、通信機能を持つ機器に設けられるデバイス認証装置であって、認証データを生成する生成手段と、前記生成手段により生成した前記認証データを可搬型の記録媒体に記録する認証データ記録手段と、前記記録媒体に記録された前記認証データを記録する記録手段と、前記記録手段により記録された前記認証データを用いて、前記可搬型の記録媒体から前記認証データを読み込んだ他の機器との間で相互認証処理を行なう認証手段とを具備したことを特徴とする。

#### 【0011】

#### 【発明の実施の形態】

以下、図面を参照して本発明の実施の形態について説明する。

本実施形態におけるデバイス認証装置は、例えば著作権保護機能等のライセンス技術を必要とする機器間の相互認証処理において、相互認証処理に必要とする認証データを可搬型のセキュアな記録媒体（SD（Secure digital）カード（登録商標）、メモリースティック（登録商標）等）を介してオフラインで提供し、このオフラインで提供された認証データを用いた相互認証処理を実行することで、機器がライセンス技術に準拠しているだけでなく、事前に認証データが提供された特定の機器だけが接続可能となるようにする。なお、本発明は、例えば著作権保護機能等のライセンス技術を必要とする機器間に限らず、ライセンス技術を必要としない機器間においても適用することができる。

#### 【0012】

図1は本実施形態に係わるデバイス認証装置10、12（12a、12b、12c）、14の使用形態の一例を示す図である。本実施形態におけるデバイス認証装置10、12（12a、12b、12c）、14は、例えば半導体メモリ、CD-ROM、DVD、磁気ディスク等の記録媒体に記録されたプログラムを読

み込み、このプログラムによって動作が制御されるコンピュータによって実現される。

#### 【0013】

図1において、デバイス認証装置10は、例えばデジタルコンテンツを、ライセンスされた特定の他の機器に対して無線通信によって提供するサーバ（コンピュータ）によって実現される。以下、デバイスA10（認証機器）として説明する。また、デバイス認証装置12（12a, 12b, 12c）, 14は、デバイスA10（サーバ）から提供されるデジタルコンテンツを受信するクライアント機器（コンピュータ）によって実現される。ただし、本実施形態において、デバイス認証装置12（12a, 12b, 12c）, 14は、デバイスA10との間の認証処理によりライセンスされた機器であることが確認されるだけでなく、可搬型の記憶媒体であるセキュアメモリカード16を用いてオフラインで取得された認証データを用いた相互認証処理によって、デジタルコンテンツの利用が許可された特定の機器であることが確認される必要がある。

#### 【0014】

例えば、図1において、デバイスA10は、相互認証処理に用いる認証データを生成してセキュアメモリカード16に書き込む。例えば、建物H1内に設置されたクライアント機器12a, 12bに対して、セキュアメモリカード16を介して認証データを提供することで、クライアント機器12a, 12bに対してコンテンツを利用させることができる。この場合、クライアント機器12cは、セキュアメモリカード16を介して認証データを取得していないので、建物H1に設置されていてもコンテンツを利用することができない。同様にして、建物H2内に設置されたクライアント機器14は、デバイスA10との間で無線通信が可能な範囲に設置されていても、セキュアメモリカード16を介して認証データを取得していなければコンテンツを利用することができない。以下、デバイスA10からセキュアメモリカード16を介して認証データがされるクライアント機器12a, 12bをデバイスB12（被認証機器）として説明する。

#### 【0015】

図2は、図1に示すデバイスA10とデバイスB12の構成を示すブロック図

である。図2に示すように、デバイスA10（サーバ）は、CPU20、ROM21、RAM22、カードスロット23、記憶装置24、EEPROM（Electrically Erasable and Programmable ROM）25、乱数発生部26、通信ユニット27、生体情報入力装置28の他、図示していない表示装置（LCD（Liquid Crystal Display）など）や入力装置（キーボード、マウスなど）等の一般的なコンピュータに設けられる機能を有している。

#### 【0016】

CPU20は、ROM21またはRAM22に記録されたプログラムを実行することで各種の処理を実行するもので、例えばROM21に記録された認証プログラム30により通信相手とする他の機器（デバイスB12など）との相互認証を実行し、ライセンスされた機器であり、かつ予め通信が許可された機器であることを判別する。また、相互認証された他の機器に対して、記憶装置24に記録されたデジタルコンテンツを提供するコンテンツサーバとして機能させる。CPU20は、認証プログラム30を実行することによって、セキュアメモリカード16に書き込んだ認証データを取得したデバイスB12との間で、認証データを用いて相互認証処理を実行する。認証プログラム30では、相互認証処理の対象とする他の機器（デバイスB12）で実行される認証プログラム32（後述する）と同じ関数に従う演算が可能である。

#### 【0017】

ROM21は、プログラムやデータが記録されるもので、他の機器の間で相互認証を行なう認証プログラム30を含む。

#### 【0018】

RAM22は、プログラムやデータが記録される。

#### 【0019】

カードスロット23は、可搬型の記録媒体に対してデータの読み込み／書き込みを実行する。カードスロット23は、例えばSDカードなどの、記録されたデータの正当性が保証されるセキュアメモリカード16を扱うものとする。

#### 【0020】

記憶装置24は、プログラムやデータが記録される。デバイスA10がデジタ

ルコンテンツのサーバとして使用される場合には、コンテンツデータが蓄積される。

【0021】

EEPROM 25 は、不揮発性の記録媒体であり、例えば認証プログラム 30 により生成された認証データが記録される。

【0022】

乱数発生部 26 は、他の機器（デバイス B 12）との間で相互認証処理を実行する際に必要となる乱数を生成する。

【0023】

通信ユニット 27 は、他の機器と通信を行なうもので、無線通信の他、ケーブルを介した通信を行なう。

【0024】

生体情報入力装置 28 は、生体情報（バイオメトリクス情報）を入力するもので、例えば指紋、掌紋、虹彩、網膜、掌などの静脈、声紋などのパターンデータを入力することができる。生体情報入力装置 28 により入力された生体情報は、認証データの生成に用いられる所有者データとして扱われる（第 2 実施形態）。

【0025】

デバイス B 12（クライアント）は、図 2 に示すように、CPU 20、ROM 21、RAM 22、カードスロット 23、記憶装置 24、EEPROM 25、乱数発生部 26、及び通信ユニット 27 を有している。なお、デバイス A 10 と同等の機能部分について同一符号を付して説明を省略する。

【0026】

デバイス B 12 の ROM 21 には、デバイス A 10 との間で相互認証をするための認証プログラム 32 が記録されているものとする。CPU 20 は、認証プログラム 32 を実行することによって、セキュアメモリカード 16 から読み込んだ認証データを用いて、セキュアメモリカード 16 に対して認証データを書き込んだデバイス A 10 との間で相互認証処理を実行する。認証プログラム 32 では、相互認証処理の対象とする他の機器（デバイス A 10）で実行される認証プログラム 30 と同じ関数に従う演算が可能である。

## 【0027】

なお、図2において、デバイスA10とデバイスB12のROM21に記録された認証プログラム30、32により認証処理を実行するものとして説明しているが、記憶装置24に記録された認証プログラムをRAM22にロードして実行されるとしても良い。記憶装置24に記録された認証プログラムは、他の記録媒体(CD-ROMなど)か読み込まれて記録されても良いし、通信ユニット27による通信によって受信して記録されても良い。

## 【0028】

## (第1実施形態)

次に、第1実施形態の動作について説明する。

図3は、デバイスA10とデバイスB12との間で行われる手続きのシーケンスを示す図、図4はデバイスA10における相互認証処理の動作を説明するためのフローチャート、図5はデバイスB12における相互認証処理の動作を説明するためのフローチャートである。デバイスA10とデバイスB12は、両方の機器ともに共通なライセンス技術を使用している。

## 【0029】

まず、デバイスA10は、認証を開始する前に、通信相手とする機器が正しいライセンス機器であるかどうかを判断するだけでなく、例えばデジタルコンテンツの利用を認めた機器であるかどうかを判断するために用いる認証データを生成する。すなわち、デバイスA10は、認証プログラム30を実行することで、乱数発生部26において乱数(乱数Cとする)を生成させ(ステップA1)、この乱数Cをもとに他の機器との間で実行される相互認証処理に用いる認証データを生成し、EEPROM25に記録しておく(ステップA2)。なお、第1実施形態では、認証データは乱数Cのデータそのものとする。

## 【0030】

デバイスA10は、EEPROM25に記録した認証データを、カードスロット23を通じてセキュアメモリカード16に書き込む(ステップA3)。

## 【0031】

デバイスA10により生成された認証データ(乱数C)は、セキュアメモリカ

ード16を介してオフラインでデバイスB12、すなわち図1中に示す特定のクライアント機器12a, 12bにのみ渡される(図3、S11)。デバイスB12は、カードスロット23に装着されたセキュアメモリカード16から、デバイスA10において生成された認証データを読み込み、EEPROM25に記録しておく(図5、ステップB1)。

#### 【0032】

デバイスA10において生成された認証データは、物理的な可搬型の記録媒体であるセキュアメモリカード16を介してデバイスB12に提供されるため、不特定の機器において取得されるおそれがない。また、セキュアメモリカード16を用い手いるため記録された認証データの正当性が保証されている。また、1枚のセキュアメモリカード16によって、コンテンツの利用を許可しようと意図する複数の機器に対して認証データを提供できる。また、デバイスB12は、セキュアメモリカード16から認証データを読み込んで記憶した後は、セキュアメモリカード16をカードスロット23に装着しておく必要はない。

#### 【0033】

こうして、デバイスA10により生成された認証データがデバイスB12に提供された後に、デバイスA10とデバイスB12との間で相互認証処理が実行可能となる。

#### 【0034】

認証を開始するデバイスA10は、乱数発生部26により乱数Aの生成を行ない、通信相手であるデバイスB12に対して通信ユニット27から送信して(challenge-A、S12)認証要求をする(ステップA4)。

#### 【0035】

デバイスB12は、デバイスA10からのchallenge-A、すなわち認証要求(乱数A)を受信すると(ステップB2)、デバイスA10から取得した乱数Aを記録しておく。また、デバイスB12は、challenge-Aを送信してきた相手が正しい機器であるかどうかを確認するため、乱数発生部26により乱数Bを生成して、challenge-Aの送信デバイスであるデバイスA10へ送信する(challenge-B、S13)(ステップB3)。

## 【0036】

デバイスA10は、challenge-B (S13)を受信すると(ステップA5)、challenge-Bで送信されてきた、デバイスB12で生成された乱数Bを用いて、認証プログラム30に従う関数Fを演算し(ステップA6)、この演算結果のデータをデバイスB12へ送信する(response-B、S14)(ステップA7)。

## 【0037】

デバイスB12は、デバイスA10から送信されてきたresponse-Bを受信し(ステップB4)、デバイスA10の確認を行なう(ステップB5)。すなわち、デバイスB12は、デバイスA10に送信した乱数Bを用いて、認証プログラム32に従う関数Fを演算し、その演算結果とデバイスA10から受信した演算結果が一致するかを判別する。ここで、演算結果が一致した場合に、デバイスA10からの正しいresponse-Bであると確認する。

## 【0038】

次に、デバイスB12は、デバイスA10からのchallenge-Aが正しい認証要求であることが確認できたので、先にデバイスA10から受信した乱数Aの値と、セキュアメモリカード16を介してオフラインにて取得した乱数Cを用いて関数Fを演算し(ステップB6)、演算結果をデバイスA10へ送信する(response-A、S15)(ステップB7)。

## 【0039】

デバイスA10は、デバイスB12から送信されてきたresponse-Aを受信し(ステップA8)、デバイスB12の確認を行なう(ステップA9)。すなわち、デバイスA10は、デバイスB12に送信した乱数Aとセキュアメモリカード16を介して提供した乱数C(EEPROM25に記録した認証データ)とを用いて、認証プログラム30に従う関数Fを演算し、その演算結果とデバイスB12から受信した演算結果が一致するかを判別する。ここで、演算結果が一致した場合に、デバイスB12からの正しいresponse-Aであると確認する。これにより、乱数AでデバイスB12が正しいライセンス機器であることを確認でき、また乱数Cで更にデバイスB12がデバイスA10から事前に承認されたデバイス

であることを確認できる。

#### 【0040】

デバイスA10において、正しいresponse-Aであることが判断されると、認証されたデバイス間で有効なセッションキーを共有することが可能となる。従って、デバイスB12は、例えばデバイスA10から送信される暗号化されたデジタルコンテンツを、キーを用いて復号化して利用することができる。

#### 【0041】

このようにして、デバイスA10により生成された認証データ（乱数C）がセキュアメモリカード16を介してデバイスB12に提供され、この認証データを用いてデバイスA10とデバイスB12との間で相互認証処理が実行される。従って、セキュアメモリカード16から認証データを取得していないクライアント機器では、デバイスA10と通信可能であり、またライセンスされた機器であったとしても、デバイスA10により認証されない。このため、デバイスA10から提供されるコンテンツを利用することができない。

#### 【0042】

##### （第2実施形態）

第1実施形態では、デバイスA10において認証データを生成する場合、乱数発生部26によって生成した乱数Cを用いているが、デバイスA10を管理する例えば所有者に関するデータを用いて認証データを生成する。

#### 【0043】

第2実施形態では、図4に示すフローチャートのステップA1、A2に代えてステップA11、A12を実行する。

#### 【0044】

デバイスA10は、他の機器との相互認証に用いる認証データを生成する場合、所有者に対して所有者データの入力进行要求する。所有者データは、デバイスA10の管理者個人を客観的に特定することが可能なデータであり、例えば管理者個人から取得されるバイオメトリクス情報（生体情報）や、第3者によって管理者個人に固有のものであることが保証される情報、例えばクレジットカード番号、銀行口座番号などの情報を用いることができる。



## 【0045】

例えば、デバイスA10は、認証データに生体情報を用いる場合、生体情報入力装置28から生体情報（例えば指紋パターン）を入力し、この生体情報を所定の形式のデータに変換して認証データとする（ステップA11, A12）。

## 【0046】

なお、セキュアメモリカード16を介してデバイスB12に提供する認証データを生成する場合に、所有者データを用いる点以外は（ステップA11, A12）、第1実施形態と同様の処理が実行されるものとして説明を省略する（ステップA3～A9）。

## 【0047】

図6には、デバイスA10に入力される所有者データが、管理者個人に固有のものであることを第3者によって保証させるためのシステム構成を示している。

## 【0048】

例えば、所有者データとしてクレジットカード番号を用いる場合、図6に示すように、デバイスA10は、インターネットなどのネットワーク40を介して、クレジットカード会社のサーバ42と接続する。デバイスA10は、認証データとして用いる所有者データ（クレジットカード番号）が入力された場合、ネットワーク40を介してサーバ42に問い合わせをする。サーバ42への問い合わせでは、例えば、入力されたクレジットカード番号と、予めサーバ42に登録されている管理者本人しか知り得ないIDやパスワード、氏名、住所などの個人データを管理者に入力させて送信する。サーバ42は、個人データに対応づけて登録してあるクレジットカード番号と、デバイスA10から初心したクレジットカード番号とを比較し、一致した場合に、管理者によって入力されたクレジットカード番号が正当であることをデバイスA10に応答する。デバイスA10は、サーバ42によって入力されたクレジットカード番号が正当であることが保証された場合に、認証データとして用いて、セキュアメモリカード16に書き込んで、他の機器に対して提供する。

## 【0049】

このようにして、セキュアメモリカード16を介してデバイスB12に提供す

る認証データに、デバイスA10の管理者個人を特定できる所有者データを用いることで、デバイスA10の管理者によって不特定の機器に認証データが提供されることを防ぐことができる。すなわち、認証データを提供することは、管理者個人のデータを他者に提供することになるので、管理者がセキュアメモリカード16を不特定の相手に渡したり、他者に無断で使用されることがないように慎重に扱うことが期待できる。このため、デバイスA10の管理者が認めた特定の機器（デバイスB12）においてのみ、デバイスA10から提供されるコンテンツを利用させることができる。

#### 【0050】

なお、前述した説明では、所有者データをそのまま認証データとして用いるものとして説明しているが、入力された所有者データに所定の処理を施したデータに変換して用いることも可能である。

#### 【0051】

##### （第3実施形態）

第3実施形態では、デバイスA10からデバイスB12に対して提供する認証データに、認証データの有効期間を示す有効期間回数データを含める。図7（a）には、デバイスA10においてセキュアメモリカード16に記録される認証データを示している。

#### 【0052】

デバイスA10は、所有者データを生成する場合、第1実施形態のように乱数Cを生成する、あるいは第2実施形態のように所有者データを入力する（ステップA1、A11）。以下の説明では、乱数Cを用いるものとして説明する。

#### 【0053】

また、デバイスA10は、有効期間データを生成し、この有効期間データと乱数Cまたは所有者データによって認証データを生成し（図7（a））、（ステップA2、A12）、セキュアメモリカード16に書き込む。有効期間データは、デバイスA10の管理者によって入力装置から入力された有効期間に応じて生成されても良いし、認証プログラム30において予め決められていても良い。有効期間データによって、認証データの有効期間を、例えば1週間、1カ月のように指

定することができる。また、有効期間は、デバイスA10において認証データが生成されてからの期間に対するものでも良いし、デバイスB12においてセキュアメモリカード16から読み込まれて記憶されてからの期間に対するものでも良い。

#### 【0054】

図8はデバイスB12における相互認証処理の動作を説明するためのフローチャートである。

#### 【0055】

デバイスA10により生成された認証データは、セキュアメモリカード16を介してオフラインでデバイスB12、すなわち図1中に示す特定のクライアント機器12a, 12bにのみ渡される。デバイスB12は、カードスロット23に装着されたセキュアメモリカード16から、デバイスA10において生成された認証データを読み込み、EEPROM25に記録しておく(図8、ステップC1)。また、デバイスB12は、セキュアメモリカード16から読み込んだ、認証データに対する有効期間データをEEPROM25に記録しておく(ステップC2)。

#### 【0056】

なお、図8に示すステップC3～C6の処理については、図5のフローチャートに示すステップB2～B5の処理と同様にして実行されるものとして説明を省略する。

#### 【0057】

デバイスB12は、ステップC6の処理によって、デバイスA10が確認されると、現在、認証データの有効期間内にあるかを、EEPROM25に記録した有効期間データをもとに確認する(ステップC7)。

#### 【0058】

ここで、有効期間内であると確認できた場合、デバイスB12は、先にデバイスA10から受信した乱数Aの値と、セキュアメモリカード16を介してオフラインにて取得した乱数Cを用いて関数Fを演算し(ステップC9)、演算結果をデバイスA10へ送信する(ステップC10)(図5、ステップB6, B7と同

じ)。

#### 【0059】

一方、有効期間内にないと確認できた場合、デバイスB12は、先にデバイスA10から受信した乱数Aの値を用いて関数Fを演算し(ステップC11)、演算結果をデバイスA10へ送信する(ステップC10)。すなわち、セキュアメモリカード16を介して取得した認証データを用いずに認証処理を実行する。この場合の認証処理では、ライセンスされた機器であることが確認することができる。

#### 【0060】

なお、有効期間内にないと確認できた場合には、認証が失敗したものと扱うようにしても良い。

#### 【0061】

このようにして、認証データに有効期間データを含めることで、デバイスA10から提供するコンテンツを他の機器(デバイスB12)が期限無く使用できることを防ぎ、またコンテンツを使用できる機器が制限無く増加することを防止できる。

#### 【0062】

##### (第4実施形態)

第4実施形態では、デバイスA10からデバイスB12に対して提供する認証データに、認証データを用いた認証処理の有効実行回数を示す有効使用回数データを含める。図7(b)には、デバイスA10においてセキュアメモリカード16に記録される認証データを示している。

#### 【0063】

デバイスA10は、所有者データを生成する場合、第1実施形態のように乱数Cを生成する、あるいは第2実施形態のように所有者データを入力する(ステップA1、A11)。以下の説明では、乱数Cを用いるものとして説明する。

#### 【0064】

また、デバイスA10は、有効使用回数データを生成し、この有効使用回数データと乱数Cまたは所有者データによって認証データを生成し(図7(b)) (

ステップA2、A12)、セキュアメモリカード16に書き込む。有効使用回数データは、デバイスA10の管理者によって入力装置から入力された有効使用回数に応じて生成されても良いし、認証プログラム30において予め決められていても良い。有効使用回数データによって、認証データの有効使用回数を、例えば10回、100回のように指定することができる。

#### 【0065】

図9はデバイスB12における相互認証処理の動作を説明するためのフローチャートである。

#### 【0066】

デバイスA10により生成された認証データは、セキュアメモリカード16を介してオフラインでデバイスB12、すなわち図1中に示す特定のクライアント機器12a、12bにのみ渡される。デバイスB12は、カードスロット23に装着されたセキュアメモリカード16から、デバイスA10において生成された認証データを読み込み、EEPROM25に記録しておく(図9、ステップD1)。また、デバイスB12は、セキュアメモリカード16から読み込んだ、認証データに対する有効使用回数データをEEPROM25に記録しておく(ステップD2)。

#### 【0067】

なお、図8に示すステップD3～D6の処理については、図5のフローチャートに示すステップB2～B5の処理と同様にして実行されるものとして説明を省略する。

#### 【0068】

デバイスB12は、ステップD6の処理によって、デバイスA10が確認されると、現在、認証データを用いた認証処理の実行回数が有効使用回数内にあるかを、EEPROM25に記録した有効使用回数データをもとに確認する(ステップC7)。なお、認証データを用いた認証処理の実行回数(認証データの使用回数)は、認証データを用いた演算処理を実行する毎にカウントしている(後述するステップD10)。

#### 【0069】

ここで、有効使用回数内であると確認できた場合、デバイス B 1 2 は、先にデバイス A 1 0 から受信した乱数 A の値と、セキュアメモリカード 1 6 を介してオフラインにて取得した乱数 C を用いて関数 F を演算し（ステップ D 9）、認証データの使用回数に 1 を加算して記憶し（ステップ D 1 0）、演算結果をデバイス A 1 0 へ送信する（ステップ D 1 1）。

#### 【0070】

一方、有効使用回数内ないと確認できた場合、デバイス B 1 2 は、先にデバイス A 1 0 から受信した乱数 A の値を用いて関数 F を演算し（ステップ D 1 2）、演算結果をデバイス A 1 0 へ送信する（ステップ D 1 1）。すなわち、セキュアメモリカード 1 6 を介して取得した認証データを用いずに認証処理を実行する。この場合の認証処理では、ライセンスされた機器であることが確認することができる。

#### 【0071】

なお、有効使用回数内ないと確認できた場合には、認証が失敗したものと扱うようにしても良い。

#### 【0072】

このようにして、認証データに有効使用回数データを含めることで、デバイス A 1 0 から提供するコンテンツを他の機器（デバイス B 1 2）が無制限に使用できることを防ぐことができる。

#### 【0073】

なお、第 3 実施形態と第 4 実施形態の説明では、それぞれ有効期間データあるいは有効使用回数データの何れかを用いるものとしているが、両方を認証データに含めてセキュアメモリカード 1 6 に書き込んで、他の機器に対して提供するようにしても良い。セキュアメモリカード 1 6 を介してオフラインで認証データを取得した機器では、前述した説明のようにして、有効期間データと有効使用回数データの両方を用いて認証データの使用制限を管理する。

#### 【0074】

また、第 3 実施形態と第 4 実施形態の説明では、デバイス A 1 0 において生成された認証データを取得したデバイス B 1 2 において、有効使用回数を越えた場

合、あるいは有効期間を越えた場合には、認証データを用いた相互認証を行わないものとして説明しているが、認証データを生成したデバイス A 10 側で有効使用回数、あるいは有効期間を確認するようにしても良い。この場合、デバイス A 10 は、有効使用回数あるいは有効期間を越えたことが確認できた場合に、認証データを用いた相互認証を行わない。

#### 【0075】

##### (第5実施形態)

前述した第1～第4実施形態では、デバイス B 12 からデバイス A 10 に対して、乱数 C を用いて算出された関数 F の演算結果を送信しているが（ステップ B 6～B 7、C 9～C 10、D 9～D 11）、デバイス A 10 からデバイス B 12 に対しても乱数 C を用いて算出された関数 F の演算結果を送信することで、相互認証をより確実にする。

#### 【0076】

図 10 は、第5実施形態におけるデバイス A 10 とデバイス B 12 との間で行われる手続きのシーケンスを示す図である。なお、図 10 に示す S 23、S 24 に関する処理以外（図 3 中に示す S 13、S 14 に対応する）は、図 3 に示す処理と同様にして実行されるものとして説明を省略する。

#### 【0077】

デバイス B 12 は、デバイス A 10 からの challenge-A、すなわち認証要求（乱数 A）を受信すると、デバイス A 10 から取得した乱数 A を記録しておく。また、デバイス B 12 は、challenge-A を送信してきた相手が正しい機器であるかどうかを確認するため、乱数発生部 26 により乱数 B を生成し、この乱数 A とセキュアメモリカード 16 を介して取得した認証データ（乱数 C）とを、challenge-A の送信デバイスであるデバイス A 10 へ送信する（challenge-B、S 23）。

#### 【0078】

デバイス A 10 は、challenge-B（S 23）を受信すると、challenge-B で送信されてきた、デバイス B 12 で生成された乱数 B と、EEPROM 25 に記憶してある他の機器に対してセキュアメモリカード 16 を介して提供した認証デ

ータ（乱数C）を用いて、認証プログラム30に従う関数Fを演算し、この演算結果のデータをデバイスB12へ送信する（response-B、S24）。

#### 【0079】

デバイスB12は、デバイスA10から送信されてきたresponse-Bを受信し、デバイスA10の確認を行なう。すなわち、デバイスB12は、デバイスA10に送信した乱数Bとセキュアメモリカード16を介して取得した認証データ（乱数C）を用いて、認証プログラム32に従う関数Fを演算し、その演算結果とデバイスA10から受信した演算結果が一致するかを判別する。ここで、演算結果が一致した場合に、デバイスA10からの正しいresponse-Bであると確認する。

#### 【0080】

このようにして、第1～第4実施形態のように、デバイスB12からデバイスA10に対して、乱数Cを用いて算出された関数Fの演算結果を送信するだけでなく、デバイスA10からデバイスB12に対しても、他の機器に提供した認証データ（乱数C）を用いて算出された関数Fの演算結果を送信することで、相互認証をより確実にすることができる。

#### 【0081】

##### （第6実施形態）

第1～第5各実施形態では、デバイスA10側からデバイスB12に対して認証要求を行っているが（challenge-A）、デバイスB12からデバイスB12に対して認証要求を行なうようにしても良い。

#### 【0082】

図11は、第6実施形態におけるデバイスA10とデバイスB12との間で行われる手続きのシーケンスを示す図である。

#### 【0083】

この場合、デバイスA10において生成される認証データを、セキュアメモリカード16を介して他のデバイスB12に提供する処理については、第1実施形態（S11）と同様にして行われる物とする（S31）。

#### 【0084】



デバイスA10により生成された認証データがデバイスB12に提供された後に、デバイスA10とデバイスB12との間で相互認証処理が実行可能となる。

【0085】

認証を開始するデバイスB12は、乱数発生部26により乱数Bの生成を行ない、通信相手であるデバイスA10に対して通信ユニット27から送信して(challenge-B、S32) 認証要求をする。

【0086】

デバイスA10は、デバイスB12からのchallenge-B、すなわち認証要求(乱数B)を受信すると、デバイスB12から取得した乱数Bを記録しておく。また、デバイスA10は、challenge-Bを送信してきた相手が正しい機器であるかどうかを確認するため、乱数発生部26により乱数Aを生成して、challenge-Bの送信デバイスであるデバイスB12へ送信する(challenge-A、S33)。

【0087】

デバイスB12は、challenge-A(S33)を受信すると、challenge-Aで送信されてきた、デバイスA10で生成された乱数Aとセキュアメモリカード16を介して取得した認証データ(乱数C)を用いて、認証プログラム32に従う関数Fを演算し、この演算結果のデータをデバイスA10へ送信する(response-A、S34)。

【0088】

デバイスA10は、デバイスB12から送信されてきたresponse-Aを受信し、デバイスB12の確認を行なう。すなわち、デバイスA10は、デバイスB12に送信した乱数Aと、セキュアメモリカード16を介して他の機器に提供した認証データ(乱数C)を用いて、認証プログラム32に従う関数Fを演算し、その演算結果とデバイスB12から受信した演算結果が一致するかを判別する。ここで、演算結果が一致した場合に、デバイスB12からの正しいresponse-Aであると確認する。

【0089】

次に、デバイスA10は、デバイスB12からのchallenge-Aが正しい認証

要求であることが確認できたので、先にデバイス B 1 2 から受信した乱数 B の値（あるいは乱数 B の値とセキュアメモリカード 1 6 を介して提供した乱数 C）を用いて関数 F を演算し、演算結果をデバイス B 1 2 へ送信する（response-B、S 3 5）。

#### 【0090】

デバイス B 1 2 は、デバイス A 1 0 から送信されてきた response-B を受信し、デバイス A 1 0 の確認を行なう。すなわち、デバイス B 1 2 は、デバイス A 1 0 に送信した乱数 B（あるいは乱数 B とセキュアメモリカード 1 6 を介して取得した乱数 C）とを用いて、認証プログラム 3 2 に従う関数 F を演算し、その演算結果とデバイス A 1 0 から受信した演算結果が一致するかを判別する。ここで、演算結果が一致した場合に、デバイス A 1 0 からの正しい response-B であると確認する。これにより、乱数 B でデバイス A 1 0 が正しいライセンス機器であることを確認でき、また乱数 C で更に故知の提供元であるデバイス A 1 0 であることを確認できる。

#### 【0091】

デバイス B 1 2 において、正しい response-B であることが判断されると、認証されたデバイス間で有効なセッションキーを共有することが可能となる。従って、デバイス B 1 2 は、例えばデバイス A 1 0 から送信される暗号化されたデジタルコンテンツを、キーを用いて復号化して利用することができる。

#### 【0092】

このようにして、デバイス A 1 0 からセキュアメモリカード 1 6 を介して認証データが提供されたデバイス B 1 2 側から、デバイス A 1 0 に対して認証要求を行って相互認証処理を実行することができる。第 6 実施形態におけるシーケンスを、第 2 ～ 第 5 実施形態に適用することも可能である。

#### 【0093】

なお、前述した各実施形態の説明では、デバイス B 1 2 は、1 つのデバイス A 1 0 からの認証データ（乱数 C）を、セキュアメモリカード 1 6 を介して取得しているが、複数のデバイスからそれぞれにおいて生成された認証データを、同様にしてセキュアメモリカードから読み出して記憶しておくこともできる。

この場合、デバイス B 1 2 は、他のデバイスから認証要求があった場合に、複数の認証データから 1 つを選択して他のデバイスとの間で認証処理を実行する。そして、この認証データを用いて認証に失敗した際に、次の認証データを選択して同様に認証処理を実行する。この処理を認証が成立するまで繰り返して実行する。これにより、デバイス B は、複数の異なるデバイスとの間で、それぞれ異なる認証データを用いて相互認証をすることができる。

#### 【0094】

また、デバイス認証装置 10 は、コンピュータによって実現されるものとして、スタンドアロンタイプの単体の装置として構成することも可能である。この場合、コンピュータに接続されて使用され、コンピュータからの要求に応じて認証処理を実行する。

#### 【0095】

このようにして、著作権保護機能等のライセンスを必要とする機器間の認証処理においては、ライセンスを持った正しい機器であることを認証するだけでなく、可搬型の記憶媒体（セキュアメモリカード 16）を用いてオフラインで認証データを取得している機器を認証して、通信相手の制限を行うことが可能となる。

#### 【0096】

なお、上述した実施形態において記載した手法は、コンピュータに実行させることのできるプログラムとして、例えば磁気ディスク（フレキシブルディスク、ハードディスク等）、光ディスク（CD-ROM、DVD等）、半導体メモリなどの記録媒体に書き込んで各種装置に提供することができる。また、通信媒体により伝送して各種装置に提供することも可能である。本装置を実現するコンピュータは、記録媒体に記録されたプログラムを読み込み、または通信媒体を介してプログラムを受信し、このプログラムによって動作が制御されることにより、上述した処理を実行する。

#### 【0097】

また、本願発明は、前述した実施形態に限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で種々に変形することが可能である。更に、前記実施形態には種々の段階の発明が含まれており、開示される複数の構成要件におけ

る適宜な組み合わせにより種々の発明が抽出され得る。例えば、実施形態に示される全構成要件から幾つかの構成要件が削除されても効果が得られる場合には、この構成要件が削除された構成が発明として抽出され得る。

#### 【0098】

##### 【発明の効果】

以上詳述したように本発明によれば、認証時に使用される認証データを可搬型の記憶媒体を通してオフラインで認証機器側から被認証機器側へ相互認証処理が行なわれる前に渡すことにより、この認証データを用いて機器間で相互認証処理が実行されるので、ライセンスされた正しい機器のうち、事前に認証機器側からオフラインで認証データを取得した被認証機器だけを接続可能にすることが可能となる。

##### 【図面の簡単な説明】

【図1】 本実施形態に係わるデバイス認証装置10、12、14の使用形態の一例を示す図。

【図2】 図1に示すデバイスA10とデバイスB12の構成を示すブロック図。

【図3】 デバイスA10とデバイスB12との間で行われる手続きのシーケンスを示す図。

【図4】 デバイスA10における相互認証処理の動作を説明するためのフローチャート。

【図5】 デバイスB12における相互認証処理の動作を説明するためのフローチャート。

【図6】 デバイスA10に入力される所有者データが管理者個人に固有のものであることを第3者によって保証させるためのシステム構成を示す図。

【図7】 有効期間回数データまたは有効期間データを含む認証データの構成例を示す図。

【図8】 デバイスB12における相互認証処理の動作を説明するためのフローチャート。

【図9】 デバイスB12における相互認証処理の動作を説明するためのフ

ローチャート。

【図10】 デバイスA10とデバイスB12との間で行われる手続きのシーケンスを示す図。

【図11】 デバイスA10とデバイスB12との間で行われる手続きのシーケンスを示す図。

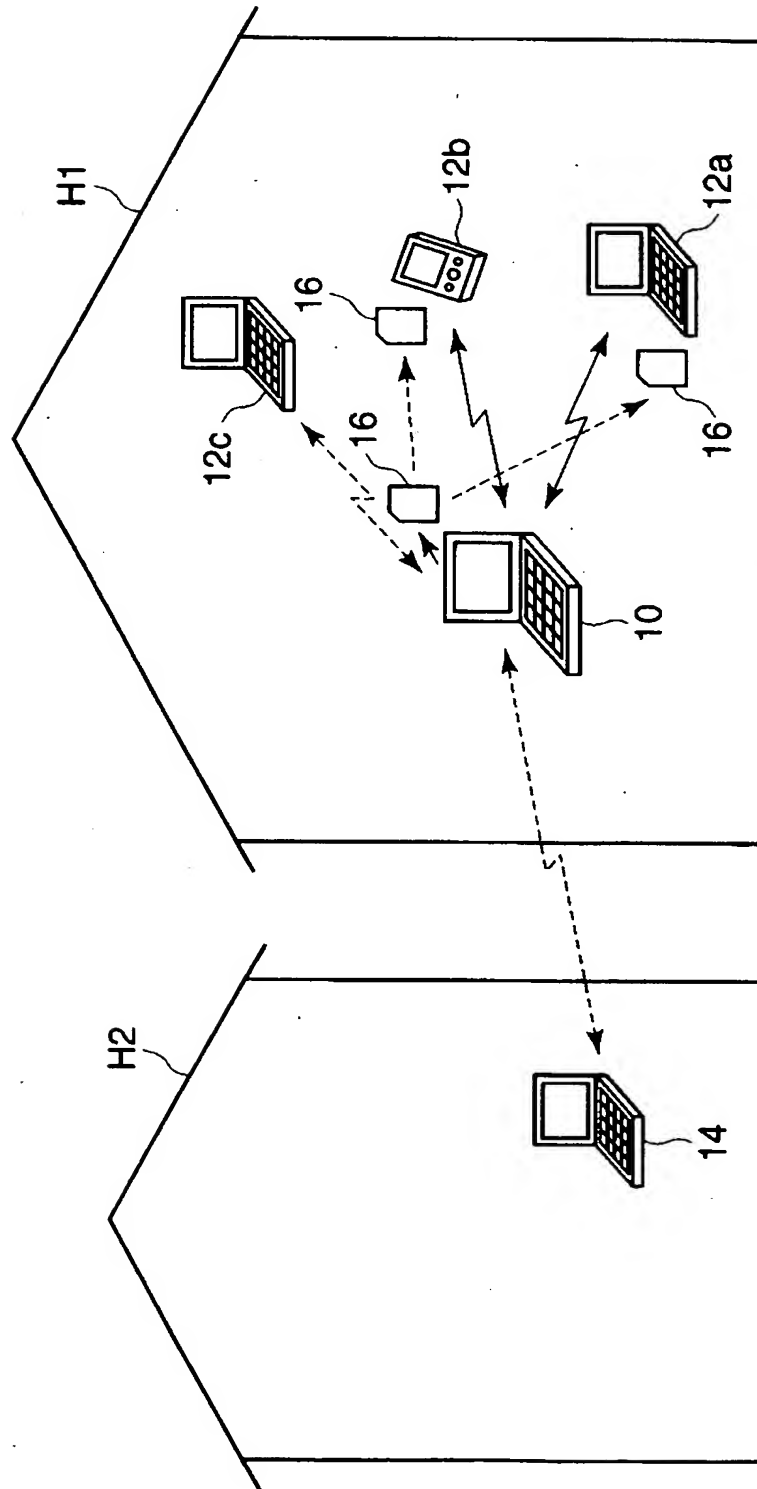
【符号の説明】

10…デバイスA、12 (12a, 12b, 12c) …デバイスB、14…デバイス、16…セキュアメモリカード、20…CPU、21…ROM、22…RAM、23…カードスロット、24…記憶装置、25…EEPROM、26…乱数発生部、27…通信ユニット、28…生体情報入力装置、40…ネットワーク、42…所有者情報認証装置。

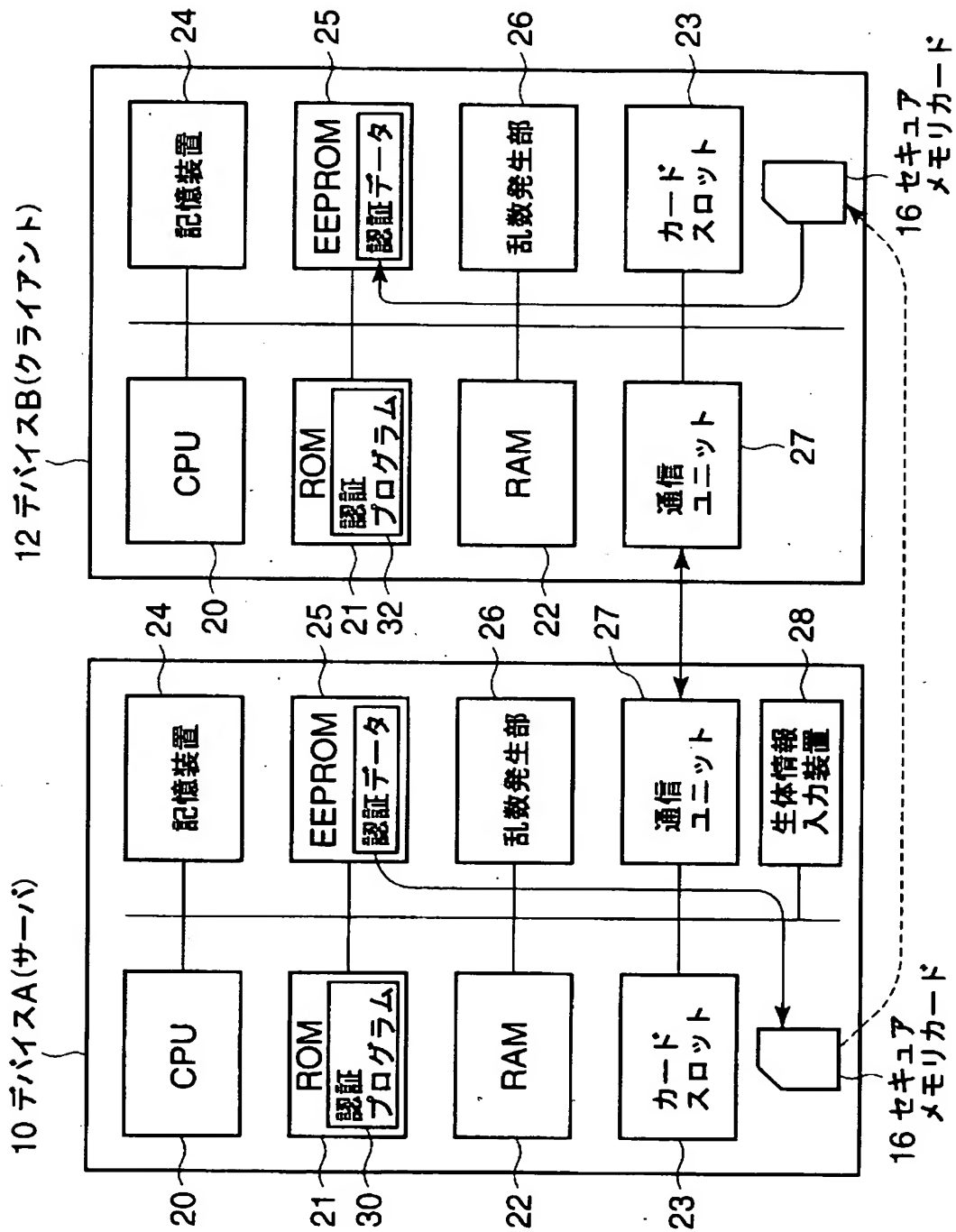
【書類名】

図面

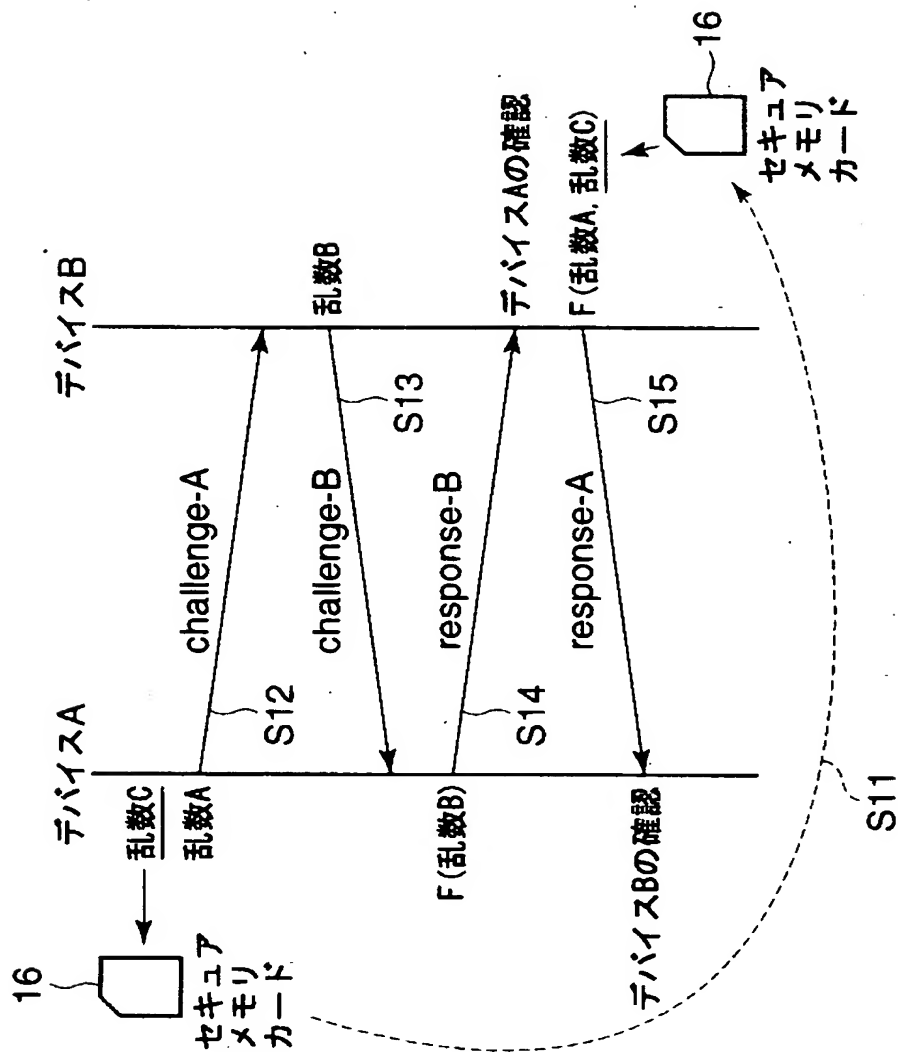
【図 1】



【図 2】

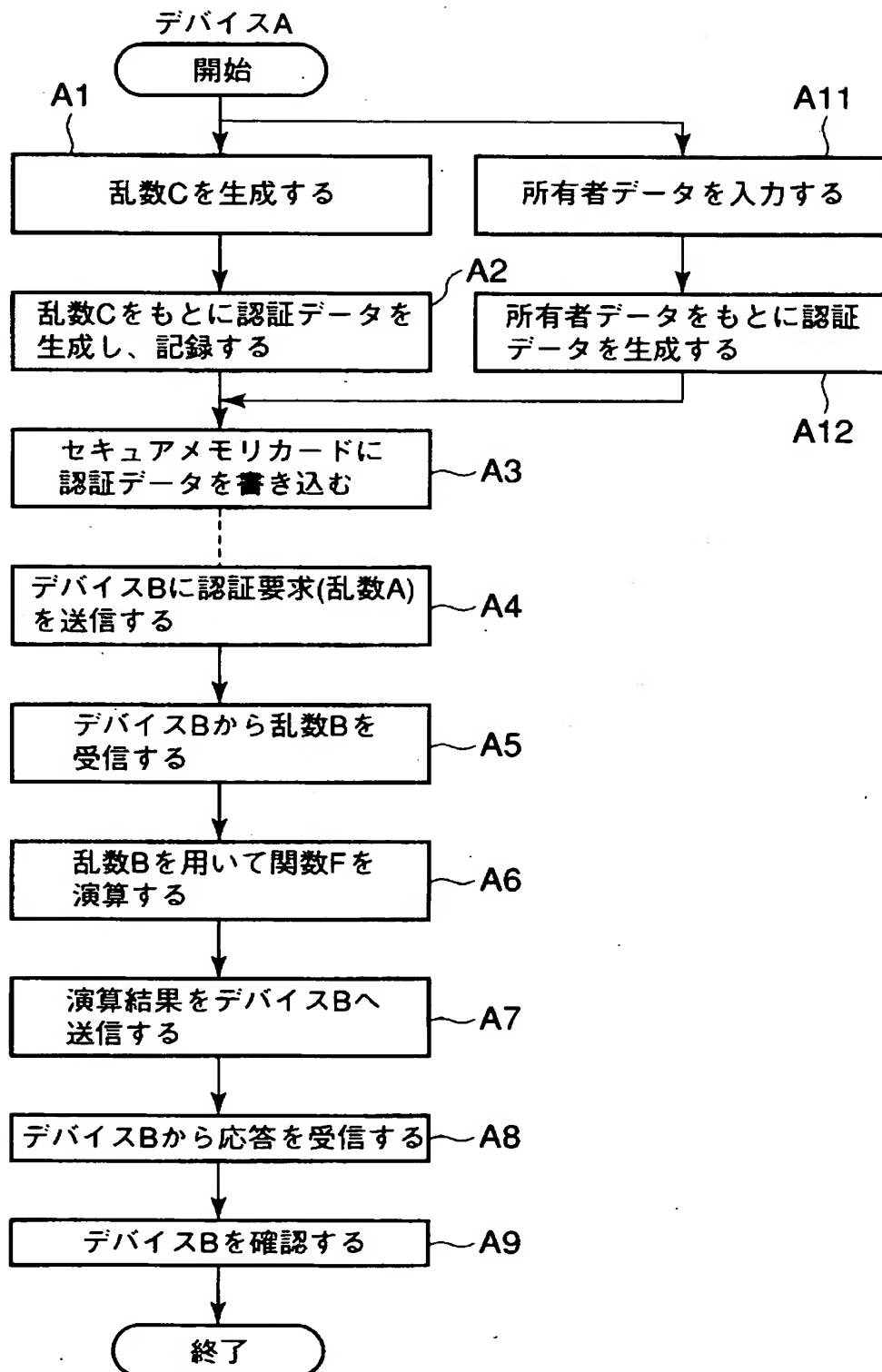


【図 3】

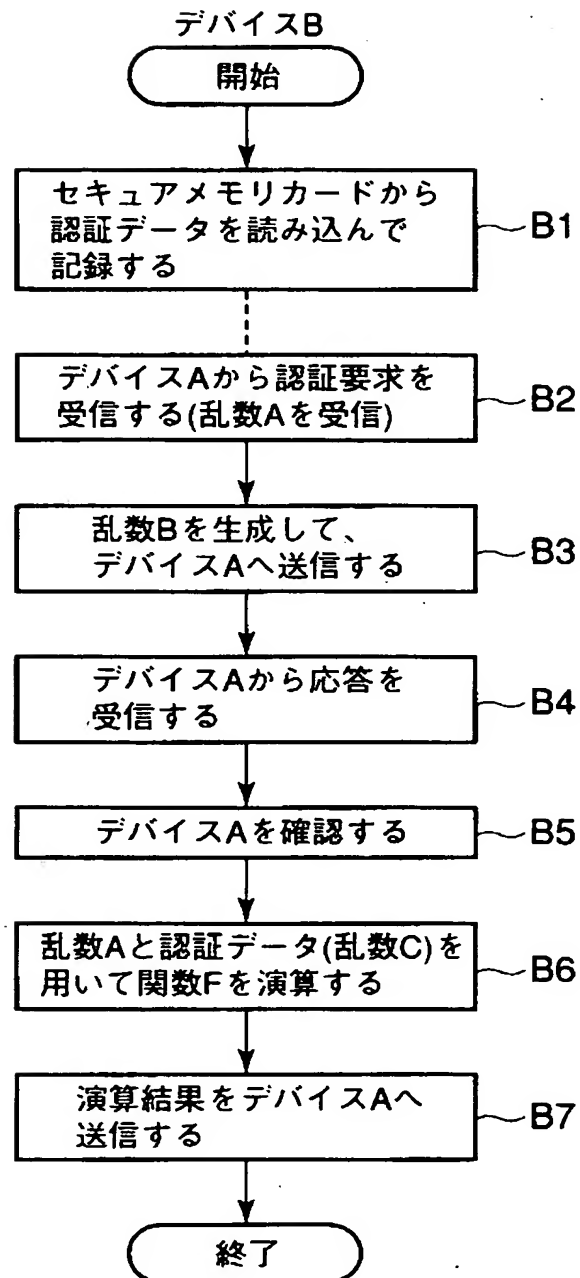




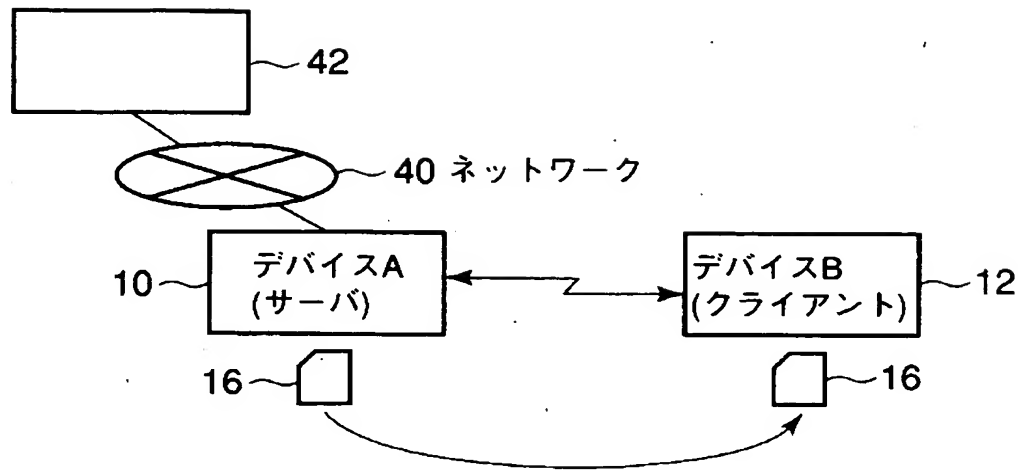
【図 4】



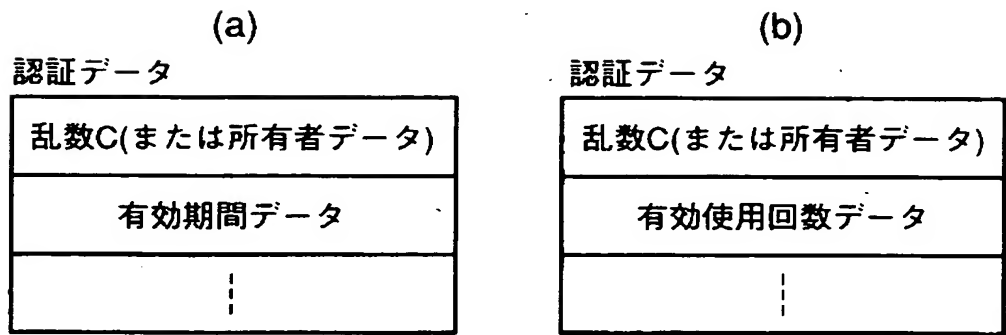
【図 5】



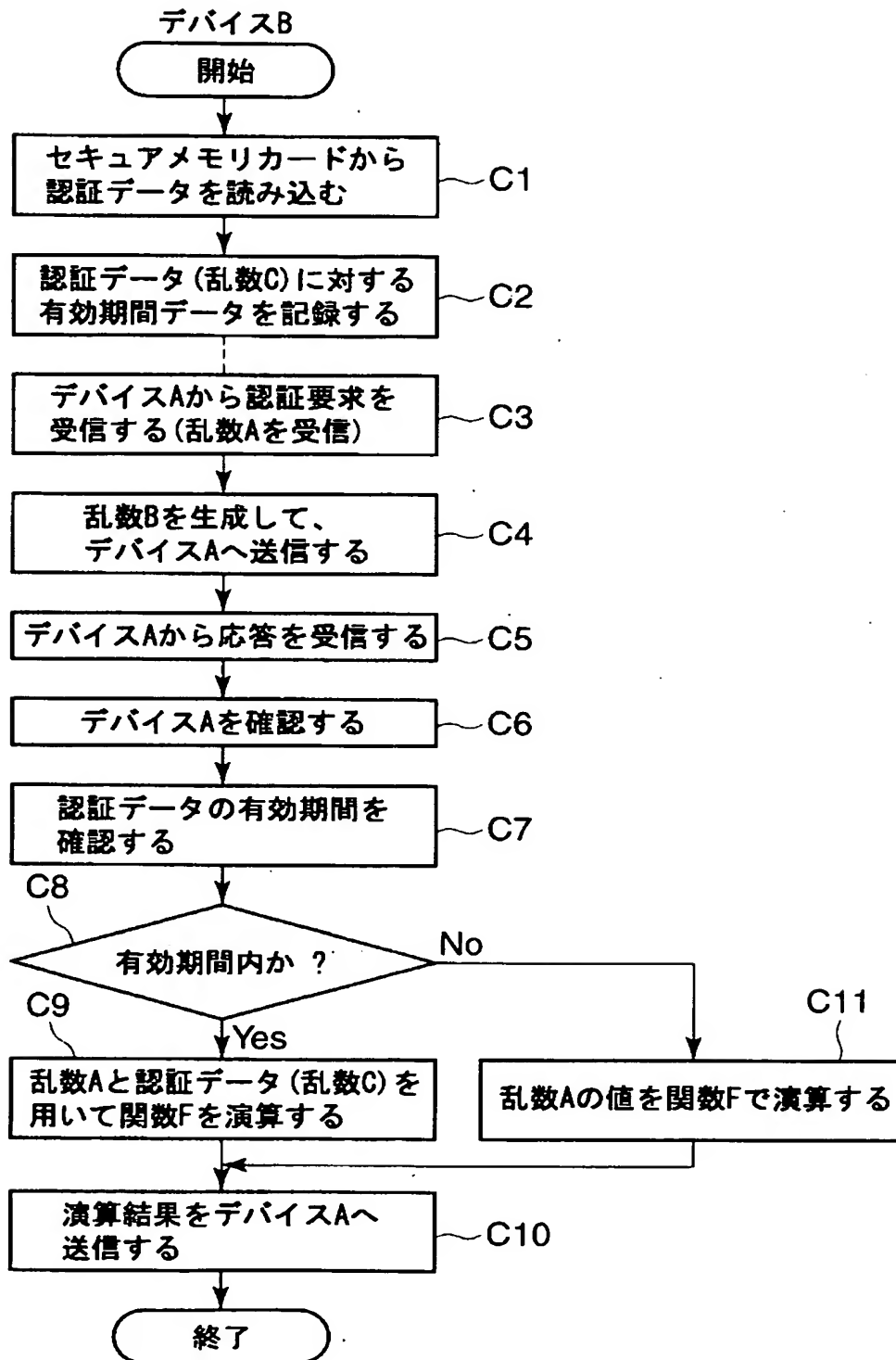
【図 6】



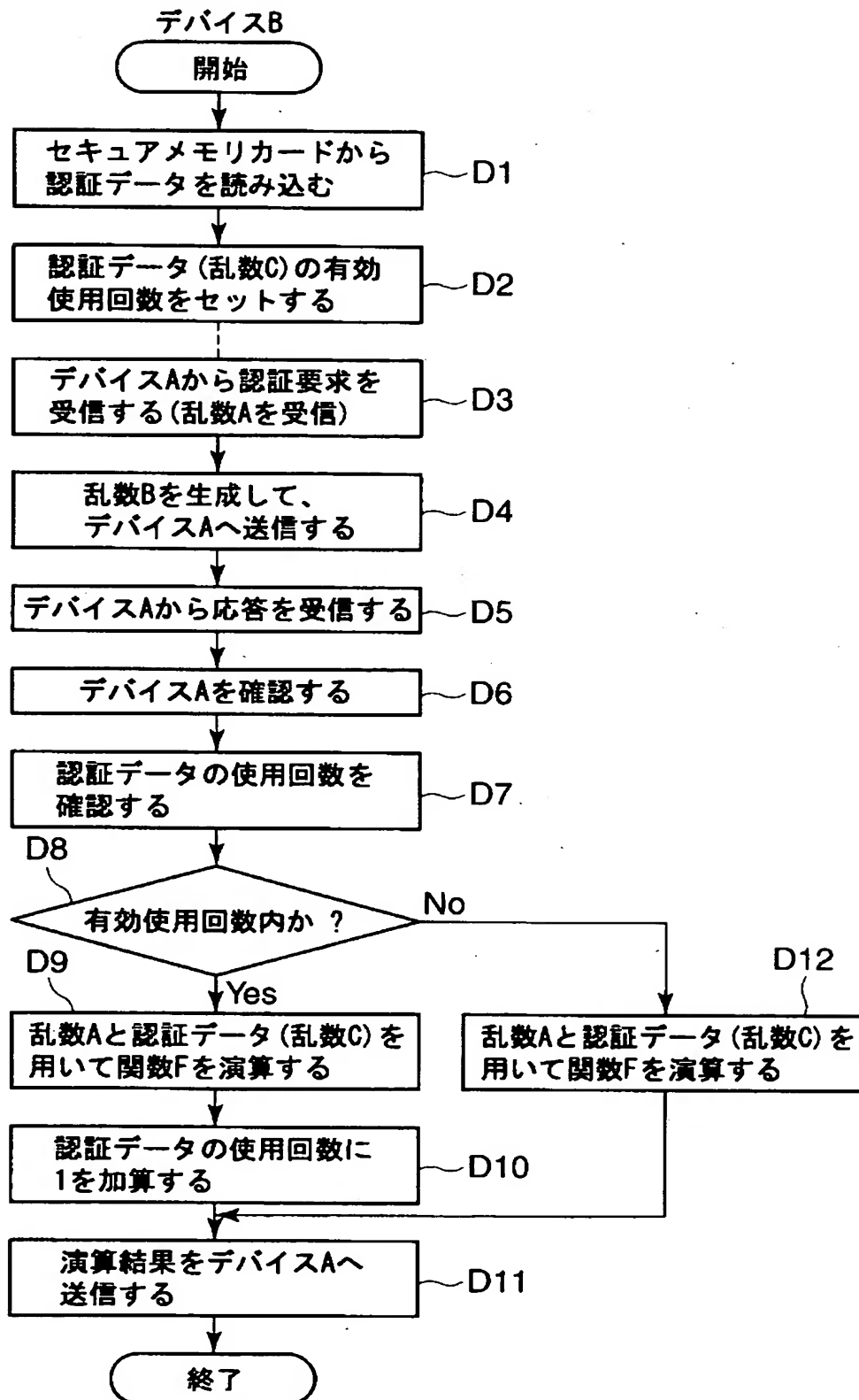
【図 7】



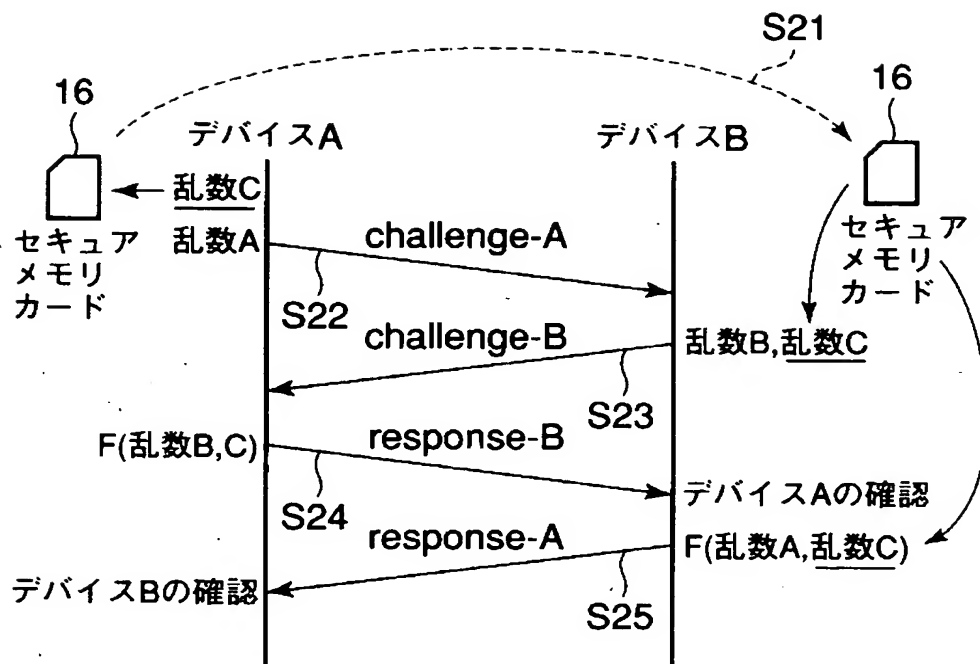
【図 8】



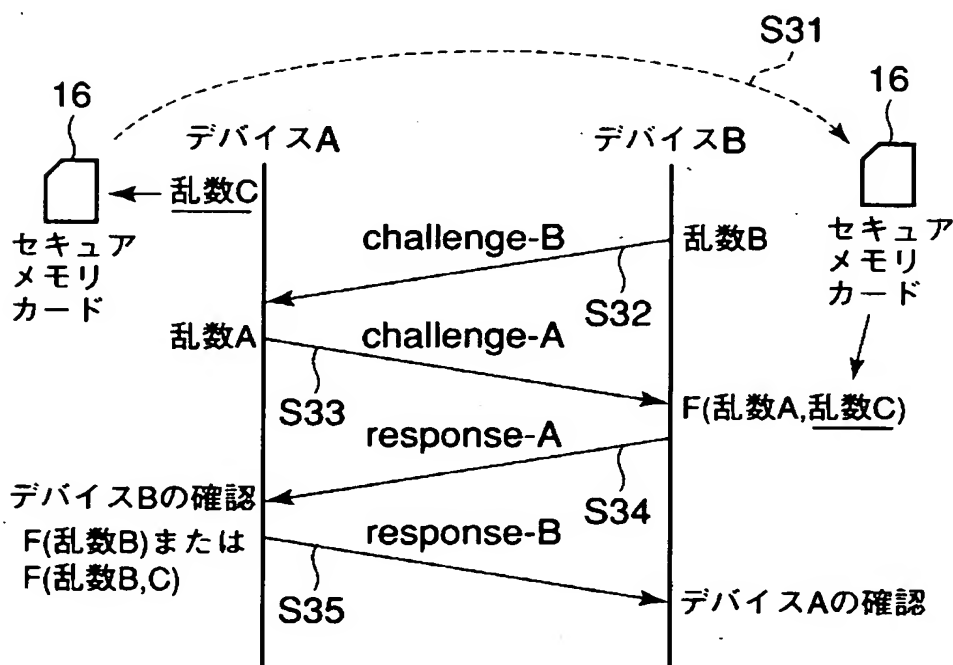
【図 9】



【図10】



【図11】



【書類名】 要約書

【要約】

【課題】 ライセンスされた正しい機器のうち、事前に認証機器側からオフラインで認証データを取得した被認証機器だけを接続可能にする。

【解決手段】 認証時に使用される認証データを可搬型の記憶媒体（セキュアメモリカード16）を通してオフラインで認証機器（デバイスA10）側から被認証機器（デバイスB12）側へ相互認証処理が行なわれる前に渡す。その後、デバイスA10とデバイスB12は、セキュアメモリカード16を介して受け渡しされた認証データを用いて相互認証処理を実行する。

【選択図】 図2

特願 2003-095671

出願人履歴情報

識別番号

[000003078]

- |          |                |
|----------|----------------|
| 1. 変更年月日 | 2001年 7月 2日    |
| [変更理由]   | 住所変更           |
| 住 所      | 東京都港区芝浦一丁目1番1号 |
| 氏 名      | 株式会社東芝         |
|          |                |
| 2. 変更年月日 | 2003年 5月 9日    |
| [変更理由]   | 名称変更           |
|          | 住所変更           |
| 住 所      | 東京都港区芝浦一丁目1番1号 |
| 氏 名      | 株式会社東芝         |